Claim Amendments

1. (Canceled).

2. (Currently Amended) The method of claim 3 [[1]] further wherein transferring comprises transferring a number of bytes specified by an operand from a memory.

3. (Currently Amended) ~~The~~ A method ~~of claim 1 further~~ comprising

configuring a cache memory of a processor to operate as a random access memory,

transferring an authenticated code module to the cache memory of the processor,

authenticating the authentic code module storing in the cache memory, and

executing the authenticated code module from the cache memory operating as a random access memory in response to determining that the authenticated code module stored in the cache memory is authentic.

~~wherein transferring comprises storing the authenticated code module in the cache memory.~~

4. (Original) The method of claim 3 further comprising invalidating the cache memory prior to storing the authenticated code module in the cache memory.

5. (Original) The method of claim 3 further comprising locking the cache memory to prevent lines of authenticated code module from being replaced.

6. (Currently Amended) The method of claim 3 [[1]] further comprising determining whether the authenticated code is authentic based upon a digital signature of the authenticated code module.

7. (Currently Amended) The method of claim 3 [[1]] further comprising

obtaining a first value from the authenticated code module stored in the ~~private~~ cache memory;

computing a second value from the authenticated code module; and

determining that the authenticated code module is authentic in response to the first value and the second value having a predetermined relationship.

8. (Currently Amended) The method of claim 3 [[1]] further comprising

retrieving a key,

decrypting a digital signature of the authenticated code module with the key to obtain a first value,

hashing the authenticated code module to obtain a second value; and

executing the authenticated code module in response to the first value and the second value having a predetermined relationship.

9. (Original) The method of claim 8 wherein

decrypting comprises using the key to RSA-decrypt the digital signature, and

hashing comprises apply a SHA-1 hash to the authenticated code module to obtain the second value.

10. (Previously Presented) The method of claim 8 further comprising retrieving the key from a processor used to execute the authenticated code module.

11. (Original) The method of claim 8 further comprising retrieving the key from a chipset.

12. (Previously Presented) The method of claim 8 further comprising retrieving the key from a token.

13. (Currently Amended) The method of claim 3 [[1]] wherein transferring comprises receiving the authenticated code module from a machine readable medium.

14. (Canceled).

15. (Currently Amended) A computing device, comprising

a chipset;

a memory coupled to the chipset;

a machine readable medium interface to receive an authenticated code module from a machine readable medium;

a private memory coupled to the chipset; and

a processor to transfer the authenticated code module from the machine readable medium interface to the private memory and to authenticate the authenticated code module stored in the private memory,

~~The computing device of claim 14,~~ wherein the chipset comprises a memory controller coupled to the memory and a separate private memory controller coupled to the private memory.

16. (Currently Amended) The computing device of claim 15 [[14]], wherein

the chipset comprises a key, and

the processor authenticates the authenticated code module stored in the private memory based upon the key of the chipset.

17. (Currently Amended) The computing device of claim 15 [[14]], wherein

the processor comprises a key and authenticates the authenticated code module stored in the private memory based upon the key of the processor.

18. (Currently Amended) The computing device of claim 15 [[14]], further comprising

a token coupled to the chipset, the token comprising a key, wherein

the processor authenticates the authenticated code module stored in the private memory based upon the key of the token.

19-21. (Canceled).

22. (Currently Amended) A computing device, comprising

a chipset;

a machine readable medium interface to receive an authenticated code module from a machine readable medium; and

a processor coupled to the chipset via a processor bus, the processor to transfer the authenticated code module from the machine readable medium interface to a private memory of the processor, to authenticate the authenticated code module stored in the private memory, and to execute the authenticated code module stored in the private memory after authenticating the authenticated code module,

~~The computing device of claim 19,~~ wherein the private memory comprises internal cache memory of the processor.

23. (Original) The computing device of claim 22, further comprises

other processors coupled to the chipset via the processor bus, wherein

the processor further locks the processor bus to prevent the other processors from altering the authenticated code module.

24. (Canceled).

25. (Currently Amended) A computing device, comprising

a memory;

a chipset comprising a memory control that defines a portion of the memory as private memory;

a machine readable medium to receive an authenticated code module from a machine readable medium; and

a processor to transfer the authenticated code module from the machine readable medium interface to the private memory and to authenticate the authenticated code module stored in the private memory,

~~The computing device of claim 24,~~ wherein the chipset comprises a memory controller coupled to the memory and a separate private memory controller coupled to the private memory.

26. (Currently Amended) The computing device of claim 25 [[24]], wherein the chipset comprises a key, and

the processor authenticates the authenticated code module stored in the private memory based upon the key of the chipset.

27. (Currently Amended) The computing device of claim 25 [[24]], wherein the processor comprises a key and authenticates the authenticated code module stored in the private memory based upon the key of the processor.

28. (Currently Amended) The computing device of claim 25 [[24]], further comprising

a token comprising a key, wherein

the processor authenticates the authenticated code module stored in the private memory based upon the key of the token.

29. (Currently Amended) A machine readable medium comprising one or more instructions that in response to being executed result in a computing device

transferring an authenticated code module to a cache memory of ~~private memory associated with~~ a processor; and

executing the authenticated code module from the cache memory ~~stored in the private memory~~ in response to determining that the authenticated code module stored in the ~~private~~ cache memory is authentic.

30. (Original) The machine readable medium of claim 29, wherein the one or more instructions in response to being executed result in the computing device

determining whether the authenticated code is authentic based upon a digital signature of the authenticated code module.

31. (Currently Amended) The machine readable medium of claim 29, wherein the one or more instructions in response to being executed result in the computing device

obtaining a first value from the authenticated code module stored in the ~~private~~ cache memory;

computing a second value from the authenticated code module; and

determining that the authenticated code module is authentic in response to the first value and the second value having a predetermined relationship.

32. (Original) The machine readable medium of claim 29, wherein the one or more instructions in response to being executed result in the computing device

retrieving an asymmetric key;

decrypting a digital signature of the authenticated code module with the asymmetric key to obtain a first value;

hashing the authenticated code module to obtain a second value; and

initiating execution of the authenticated code module in response to the first value and the second value having a predetermined relationship.

33. (Original) The machine readable medium of claim 29, wherein the one or more instructions comprises a launch instruction that in response to being executed results in the computing device

retrieving an asymmetric key;

decrypting a digital signature of the authenticated code module with the asymmetric key to obtain a first value;

hashing the authenticated code module to obtain a second value; and

initiating execution of the authenticated code module in response to the first value and the second value having a predetermined relationship.

34. (Original) The machine readable medium of claim 33, wherein the one or more instructions in response to being executed result in the computing device

receiving the authenticated code module via a machine readable medium interface.